PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 1/00 — A1

(11) International Publication Number: WO 94/06071

(43) International Publication Date: 17 March 1994 (17.03.94)

(21) International Application Number: PCT/GB93/01835

(22) International Filing Date: 27 August 1993 (27.08.93)

(30) Priority data:
9218452.2 29 August 1992 (29.08.92) GB

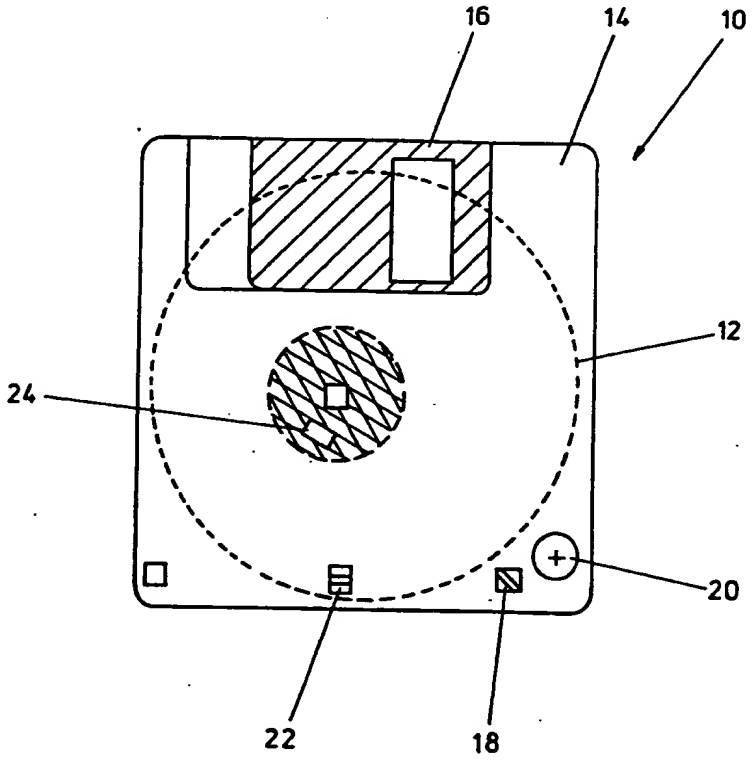
(71)(72) Applicant and Inventor: ABDULHAYOGLU, Melih [TR/GB]; 15 Town Street, Farsley, Leeds, West Yorkshire LS28 5EN (GB).

(74) Agent: JOHNSTONE, Helen, Margaret; Urquhart-Dykes & Lord, Tower House, Merrion Way, Leeds LS2 8PA (GB).

(81) Designated States: AT, AU, BB, BG, BR, BY, CA, CH, CZ, DE, DK, ES, FI, GB, HU, JP, KP, KR, KZ, LK, LU, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SK, UA, US, UZ, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: A DONGLE



(57) Abstract

A dongle comprises means in the form of for example circuitry which is adapted to be able to change the information contained in a particular memory location in a predetermined manner. Software to be protected will not run unless it identifies a predetermined pattern in a particular memory location. The memory location may be either real or virtual.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**FR**	France	**MR**	Mauritania
AU	Australia	**GA**	Gabon	**MW**	Malawi
BB	Barbados	**GB**	United Kingdom	**NE**	Niger
BE	Belgium	**GN**	Guinea	**NL**	Netherlands
BF	Burkina Faso	**GR**	Greece	**NO**	Norway
BG	Bulgaria	**HU**	Hungary	**NZ**	New Zealand
BJ	Benin	**IE**	Ireland	**PL**	Poland
BR	Brazil	**IT**	Italy	**PT**	Portugal
BY	Belarus	**JP**	Japan	**RO**	Romania
CA	Canada	**KP**	Democratic People's Republic of Korea	**RU**	Russian Federation
CF	Central African Republic			**SD**	Sudan
CG	Congo	**KR**	Republic of Korea	**SE**	Sweden
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovak Republic
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LU**	Luxembourg	**TD**	Chad
CS	Czechoslovakia	**LV**	Latvia	**TG**	Togo
CZ	Czech Republic	**MC**	Monaco	**UA**	Ukraine
DE	Germany	**MG**	Madagascar	**US**	United States of America
DK	Denmark	**ML**	Mali	**UZ**	Uzbekistan
ES	Spain	**MN**	Mongolia	**VN**	Viet Nam
FI	Finland				

A DONGLE

This invention relates to a method for preventing use of unauthorised copies of software and to a protected recording medium, unauthorised copies of which are rendered useless.

The invention also provides a communication link between any device using a memory, whether physical or virtual, and also provides security for such a device. The invention is thus useful for protecting software and also the confidentiality of certain data.

The use of magnetic recording media such as diskettes to record computer programmes has become very widespread in recent years. Conventional diskettes are easily copied and this leads to the problem that unauthorised copies can be widely disseminated thus depriving the software copyright owner from his rightful fees or royalties.

It has been proposed to prevent copying of information from diskettes by encoding on them instructions which normally prevent the writing of the contents of the diskette onto another disk or diskette. However, what can be protected by software can be changed by software and sophisticated copiers can circumvent such protection.

Another approach to software protection is the use of some sort of circuitry plugged into one of the computer ports and having a communication between itself and the software thereby providing security for the software since the latter could not be activated without communicating with this circuit. The latter is known as a "Dongle". However, the use of a conventional dongle is not generally favoured especially because it is inconvenient for the user who must place the required circuitry into a computer port or bus slot. Moreover, where several different types of software are employed each needing a different dongle, the computer user may need to change dongles between programmes which could well cause him to use other proprietary brands of software not employing this form of protection.

In addition, such devices are never transparent and may

therefore cause problems when it is required to interface other devices such as printers, modems etc with the computer.

The invention seeks to provide an improved form of dongle for use in protecting computer software and data.

According to a first aspect of the invention there is provided a device comprising means for changing information at a particular memory location forming part of a computer system.

The device may be a dongle.

The memory may be either real or virtual.

The dongle according to the invention may comprise circuitry in the form of electronics which circuitry may be built onto a cable between a controller card (IDE, SCSI, EISA controller cards etc) and the computer hard disk.

Alternatively, the dongle forming the present invention may comprise circuitry which may be included within the hard disk controller circuitry or on the controller card (IDE, SCSI, EISA controller cards etc)or in the input/output controller thus providing a simple solution to security problems.

The present invention may be positioned on any device such as a floppy disk, game cartridge, memory card etc which comprises a memory whether physical or virtual.

The circuitry, which may be in the form of an integrated circuit, silicon chip etc may be formed to perform a mathematical algorithm. A well known algorithm is the RSA algorithm which is virtually impossible to crack. The dongle of the present invention will contain a key code on which the circuitry will perform the algorithm. The software to be protected will look for a particular code which is the output produced by the circuitry to a memory location, and once it sees this string of digits, will run the programme.

The software may be programmed to address a particular memory location in the hard disk. However, the software may also be programmed to address a location which does not actually exist on the hard disk or any other memory. In such a situation, on receipt of a signal from the software, the circuitry will emulate a memory and will produce an appropriate code using a predetermined algorithm. By means of a virtual

memory, none of the memory spaces in the hard disk is taken up with codes.

Alternatively, the means for changing information comprises a dongle which comprises a computer disk having circuitry enabling it to change the information on a particular location of the disk according to a predetermined pattern.

It will be understood that the term "disk" is used generally to include software recording media and includes magnetic tapes disks and diskettes as well as memory cards, optical disks and the like as well as hard disks.

The invention seeks to provide a transparent operation which is invisible to the user and also to other devices such as printers interfacing the computer.

The means for changing the data may comprise an integrated circuit, a read write head and a battery attached to a magnetic diskette. In addition there is provided a synchronisation point so that the integrated circuit can be synchronised with the disk drive control circuitry. The circuit targets a particular location, which may be a sector or cluster, for example sector 1, on the disk and changes the data recorded on that location each time the disk revolves according to a predetermined pattern which could be as simple as zero one zero one etc. or could be more complicated than this. The software to be protected "looks" for this changing pattern on the disk and will not respond, that is start the programme running, unless the relevant pattern is detected. Thus the disk may be used as a "key" to start the programme running.

The disk of the invention cannot be successfully copied since any attempted copy will only record one value of the location having changing information and this will not be sufficient subsequently to run the software being protected.

Where a magnetic diskette is employed, it may be activated as soon as the metal covering is open (when inserted into the computer disk drive). However, there are other methods of activating the disk for example manual, revolution caused activation, or even a key pad on the disk which may, for instance, need to have a PIN number inserted for it to be

activated. It is currently preferred to activate the disk from the opening of the metal cover after insertion into the disk drive. The disk will be directly in synchronisation with the disk drive provided this is compatible with the disk operating system of the computer.

It is possible to provide a switch or key which will cause the dongle of the invention to write to a different location on the disk. This may be useful if the particular sector on which the changing information is written on is destroyed which would otherwise render the dongle of the invention unusable. If another sector can be utilised then the life of the dongle is extended.

Exactly the same principle of operation can be used on hard disks. In this case then the floppy dongle of the invention need be used once only since the identification code of the hard disk can be transferred to the chip on the diskette only allowing that particular identified computer to use the software. Other variations or modifications can be included such as features allowing the software to be used in a different computer provided it is deleted from the previous computer, protection against accidental deletion, and the like.

In one mode of operating the invention the disk or diskette in accordance with the invention is used as a "key" every time the software is run in order to start it. This would give complete protection with simplicity provided that the hard disk is designed in accordance with the invention. Alternatively, the floppy dongle of the invention would need to remain in place as long as the software is being used.

In an alternative mode of operation, the read/write head of the disk can be in direct communication with the read/write head of the computer and information may be passed directly without passing through the magnetic or other recording medium.

The invention will now be described further, by way of example, with reference to the accompanying drawing in which:

Figure 1 is a diagrammatic view of a diskette modified in accordance with the invention;

Figures 2 to 9 are flow charts showing functions which

may be performed by means of the present invention;

Figure 10 is a schematic representation of a system including a dongle according to the present invention; and

Figure 11 is a schematic representation of a system including a communications link according to the present invention enabling an external device to communicate with a computer.

Referring to Figure 1, a magnetic computer diskette generally designated (10) comprises a disk of magnetic recording material (12) within a housing (14) having a openable metal covering (16) allowing the disk drive of the computer access to the recording medium (12). This comprises a conventional magnetic diskette. In accordance with the invention the diskette (10) additionally carries an integrated circuit (18) coupled to a battery (20) and a read write head (22). In order that the position of the recording medium (12) can be accurately known a synchronisation point (24) is also provided. It is thus possible to pick a specific sector of the recording medium (12), for example sector 1 (although any other sector or indeed sectors could be used if desired) and change the data on this sector on subsequent revolution via the read write head (22) according to information held in the integrated circuit (18). The particular pattern of change of information will be predetermined and embedded in the software which it is desired to protect so that the latter "looks for" that particular pattern and will not run unless it detects it.

In use the diskette (10) of the invention is inserted into the or one of the disk drives of the computer on which the software to be protected has already been loaded and the relevant commands to run the software are entered. The software will detect the pattern on the disk thus releasing it to run and the user can use the software. Without the diskette (10) the software will not run. Alternatively, the software can be installed using the disk. Any attempt to copy the diskette (10) will not be successful since only one value of the protected location can be copied and thus the copy will not

activate the software.

A second embodiment of the invention the dongle according to the invention comprises circuitry which may for example be built onto the cable between the controller card on controller and the hard disk. The invention makes use of a dedicated memory location in which the data within that location is changed in predetermined manner by means of the invention. The memory location effectively serves as a communication link between the device which could be a security device or any other device, and say a computer. The memory location may be either physical or virtual.

Whenever the computer requests access to the security device it wakes up the device by either addressing a particular location, so that when that particular location is addressed the device wakes up, or using any other control signals available between the memory and the computer. In the case of a hard disk, there are command and control signals or any combination thereof, which are available and can be used to wake up the device forming the invention at that particular memory location.

Once the device is awake it performs its algorithm and puts the output of the algorithm on the particular memory location. If the output is longer than the particular memory location then the device repeatedly puts segments of the algorithm into the memory location as many times as necessary, thus allowing the computer to read it in its entirety. Once the software has read the entire algorithm and has identified that it is the correct algorithm the software to be protected will run.

By means of the present invention therefore a communication link is established without the need for an extra link between the computer and a security device. This is a very useful feature, because it means that a security device according to the present invention may be installed into any computer without having to use available ports or bus slots or any other communication link. This in turn will mean that by means of the invention a standard security device can be built

to be incorporated in every computer at very little cost. In addition, due to the small size of the preferred embodiment of the invention, the device will be able to fit any computer and will effectively be transparent. This aspect of transparency is a sharp contrast to any existing devices.

Because the invention also provides a communication link between the security device according to the present invention and the computer, it can also act as an additional port or bus slot of the computer. In other words, a specially designed slot may be provided on the device according to the invention which would allow for input from other devices such as printers into the computer.

Referring to Figure 10, a system including a dongle according to the present invention is designated generally by the reference numeral 90. The system 90 comprises an input/output (I/O) controller 91, a comparator 92, a hard disk 93, a data control disable/enable device 94 and a dongle according to the present invention 95. In use, the software to be run is loaded into the computer system. This causes the I/O controller 91 to send a "wake-up" signal to the comparator. The comparator 92 checks for the wake-up signal and if it is present and correct, "wakes up" the dongle 95. The dongle 95 changes the data in a predetermined manner in accordance with an algorism programmed within it. The dongle 95 then sends the data back from the data line and tells the disable/enable device 94 that it has finished. The data is transmitted to the software, and if the data returned to the software is identified as being correct by the software, the software will run.

Referring to Figure 11, a similar system is illustrated in which the dongle 95 according to the present invention is replaced by an external device 105. The device could be for example a printer. It would be possible to have several external devices for example a printer, a modem etc positioned in series with one another. The software in the system shown in Figure 11 would be able to communicate with the external device 110 in exactly the same manner as described in respect

of communication between the software and the dongle 95 in Figure 10.

Functions which may be performed by way of the present invention will now be described in more detail. The addresses referred to have the following meanings:

X1 = When this address is addressed the Smart / Intelligent Memory Emulation Circuitry (SMEC) forming the dongle according to the present invention will start performing an algorithm. This is the start signal for the algorithm performing function.

X12 = This address will hold the secret key that is needed to perform the algorithm. So when the request is made for the algorithm this address must be read as well so that the secret key can be obtained in order to perform the function.

X2 = This is the address which will act as the enabling signal to the location locking function.

X21 = The locked location will require an authorisation code for access and this address will store it.

X22 = This address will store the start address of the location to be protected.

X23 = This address will store the ending address of the location to be protected.

X3 = This address will act as the enabling signal for the location unlocking function to start.

X4 = This address will act as the enabling signal for the Data Encryption function (activation) to start.

X41 = This address will store a value which will tell the circuitry whether an access code is required for encryption / decryption.

X42 = This address will hold the access code value for encryption.

X5 = This address will act as the enabling signal for the initial activation of data encryption mode.

X6 = This address will start the data encryption deactivation.

X7 = This address will start the selective data encryption.

X8 = This address will start the selective data encryption deactivation.

Function 1) Algorithm performing

This function is useful for software protection. A simple confirmation of the security device's existence by performing an almost uncrackable algorithm is sufficient for the software to start. The function is explained below with reference to Figure 2.

The circuit forming the dongle according to the invention "looks for" a signal which is in the form of an address of memory location (or any other control signal or combination thereof) called X1. If it detects it the circuit disables the data lines between for example the hard disk drive where the memory locator is located (any other memory device could be used such as floppy disk drive, memory card etc) and the host controller and passes it onto the Smart / Intelligent Memory Emulation Circuitry (SMEC) circuitry forming the present invention. The software then puts a value, which is to be the value of a secret key for performing the algorithm, on the address X12 and the circuitry reads this as many times as necessary in order to obtain a long key which might be up to 200 bytes long. In other words, the circuit would read the location X12 200 times. After obtaining the secret key the circuit performs the algorithm and generates an output of say 200 bytes and puts this value at address X12 for the software to read say 200 times. In other words, the software accesses this address X12 200 times. The operation is completed and, depending on the output generated by the circuitry, the software will either run or halt.

Function 2) Location protection

(a) Locking

This function is useful for protecting locations where either confidential data has been stored or software resides. The protection is provided by preventing access to the locations / areas designated therefore providing security. The function is explained below, with reference to Figures 3 and 4.

The circuit "looks for" a signal which is in the form of

an address of memory location called X2. If detected then the SMEC circuit of the present invention reads the value of X22 which stores the starting address of the location to be protected. This value is put there by the software. The SMEC circuit of the present invention then reads the value at address X23 which holds the ending address of the location, and then reads the address X21 which holds the authorisation code for accessing this location. After completing these operations the circuit will activate itself to look for the commands (anything from read / write to copy etc) relating to the memory locations and which are located in between the memory location starting address which was given by X22 and the memory locating ending address which was given by X23. If it detects the commands the circuit will ask for the authorisation code which was stored at address X21. If the code is correct it will grant access to these locations.

(b) Unlocking

The circuit of the invention looks for a signal which is in the form of an address or memory location called X3. If it detects it then it reads data at address X22, which stores the information about the starting address of the location and then reads X23, which stores the information about the ending address of the location. It then reads the data at X21, which stores the code for accessing the location and if it is correct then it deactivates the circuit.

Function 3) Data encryption (Activation)

This function is useful for storing confidential / non-confidential data in an encrypted form therefore preventing unauthorised users to gain access to the original data since it is stored in an encrypted form and does not mean anything unless the secret keys are obtained. The function is explained below with reference to Figures 5 to 7.

The circuit of the present invention "looks for" a signal which is in the form of an address or memory location called X41. If it detects the code it reads the data stored at this address, which will tell the circuit of the present invention whether to expect an access code or not depending on the value

of that address. If it requests the code, the code is stored at address X42. The circuitry will then "look for" a command defining a function to be carried out. For example the function may be to encrypt or decrypt a read / write signal. If the function relates to the write mode of the computer, the circuit forming the present invention encrypts the data and puts it into the memory. If the function relates to the read mode, then depending on any previous procedure, it either asks for an access code or not. If it requests the access code then the circuit reads the address X42 and if the value is correct it decrypts the data from the memory. If the value is incorrect, the user has 3 tries before access is denied and the system halted. If there are no access codes the data is decrypted directly.

Function 3) Data encryption (initial activation)

This initial activation is needed because once the system is invoked for data encryption, if the user tries to read a location, even though that memory location is not encrypted, the location will be decrypted therefore causing problems. Initial activation is therefore needed to initially encrypt all the data in the memory preparing it for the data encryption. When the address X5 is detected each location is read, encrypted and stored again.

Function 3) Data encryption (Deactivation)

Address X6 reads address X41, which tells the SMEC forming the present invention whether an access code is needed. If an access code is required X42 is read, and if the value is correct the data is read, decrypted and written back onto the memory. If the code is incorrect access is denied, say three times. The encryption circuit is then deactivated and remains transparent.

Function 4) Selective data encryption (activation)

This function is useful for protecting selected data by encrypting). The function is explained below with reference to Figure 8:

If address X7 check the control signals. If the control signal is a read signal then start encryption if the control

signal is a write signal start decryption and stay active.

Function 4) Selective data encryption (deactivation)

If address X8, decrypt the locations that were encrypted with selective data encryption and stay transparent (Figure 9).

The invention provides a means of security without occupying any port or bus slot therefore providing a very desirable security since it uses a memory as a communication link which would make the "standard security" a reality in computers.

The dongle of the invention is very much more easy to use than conventional dongles and provides a simple cheap and effective way of protecting software against unauthorised copying.

CLAIMS

1. A dongle comprising means for changing information at a particular memory location in a device having a memory.

2. A dongle according to claim 1 wherein the memory is a virtual memory.

3. A dongle according to claim 1 wherein the memory is a real memory.

4. A dongle according to any one of the preceding claims comprising circuitry in the form of electronics which circuitry may be built onto a cable between a control card (IDE, SCSI, EISA control card) and a computer hard disk.

5. A dongle according to amy one of claims 1 to 3 wherein the dongle comprises circuitry which may be included within a hard disk controller circuitry.

6. A dongle according to any one of claims 1 to 3 positionable on a device such as a floppy disk, game cartridge, memory card.

7. A dongle according to any one of the preceding claims comprising an integrated circuit.

8. A dongle according to any one of the preceding claims adapted to perform a mathematical algorism.

9. A system comprising a dongle as claimed in any one of the preceding claims, and further comprising software to be protected by the dongle.

10. A system according to claim 9 wherein the software is programmed to address a memory location.

11. A communication link established between a device having a memory location and any other device, which communications link comprises means for altering the information in a particular memory location in a predetermined manner.

12. A device comprising means for changing information at a particular memory location in a device having a memory.

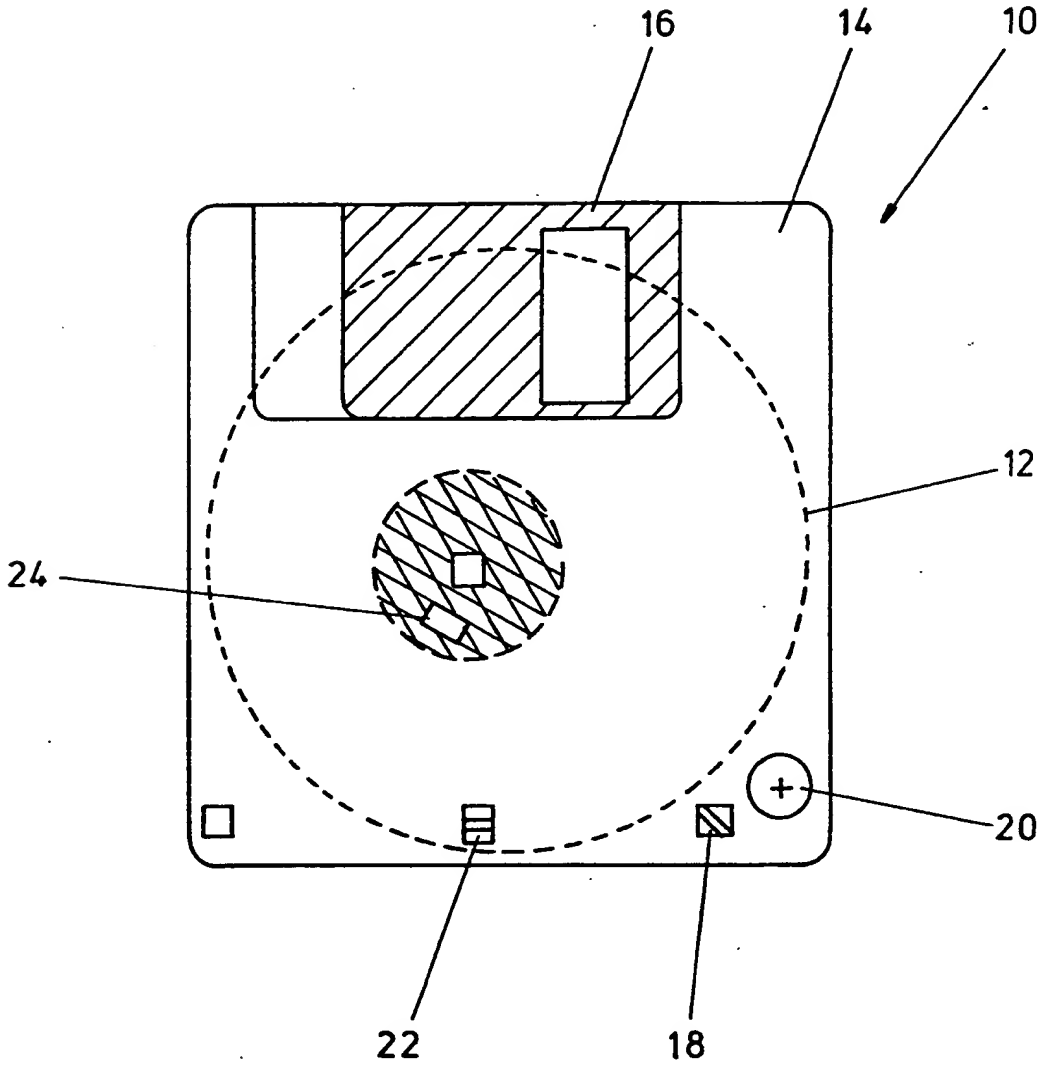
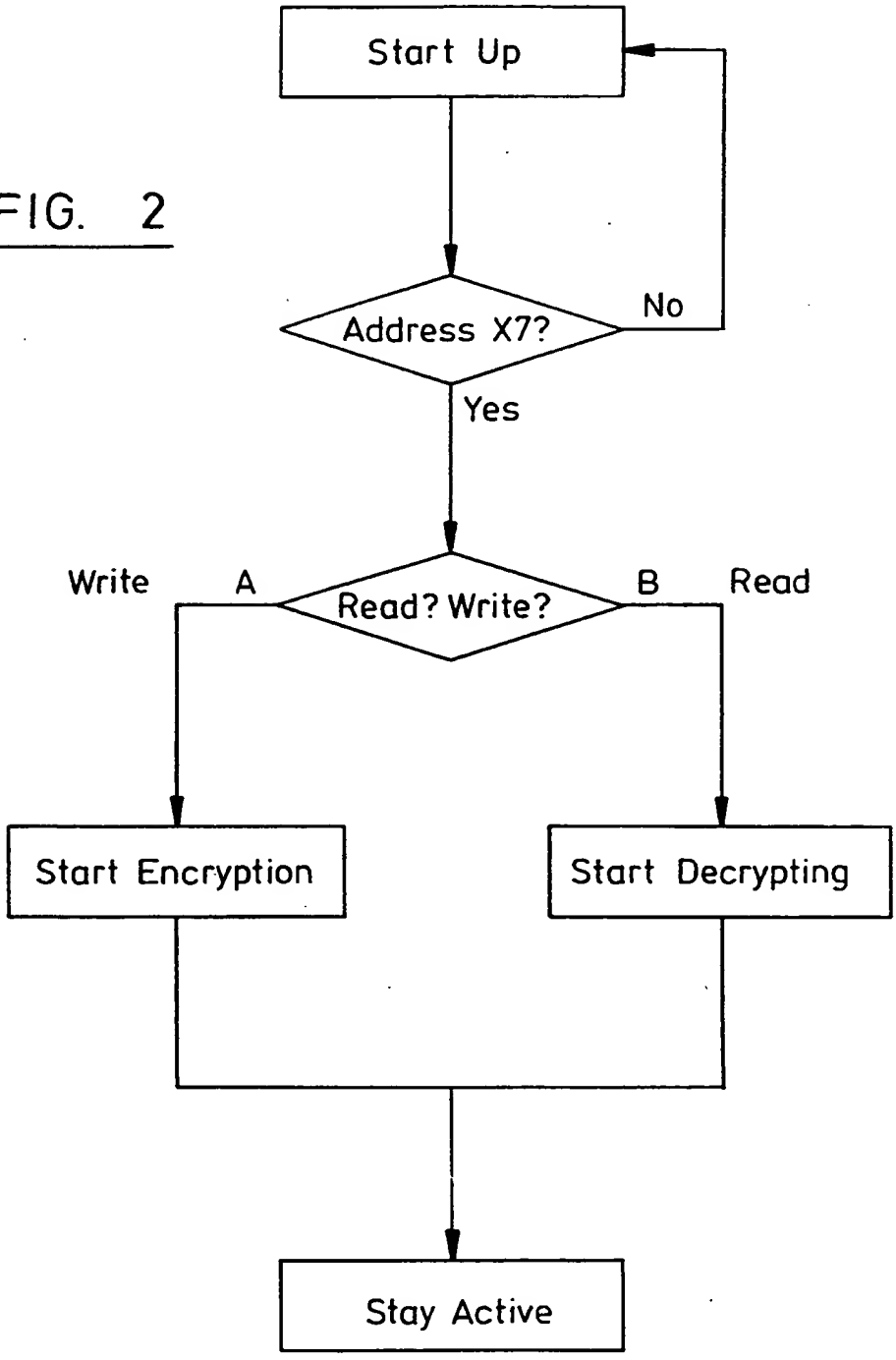


FIG. 1

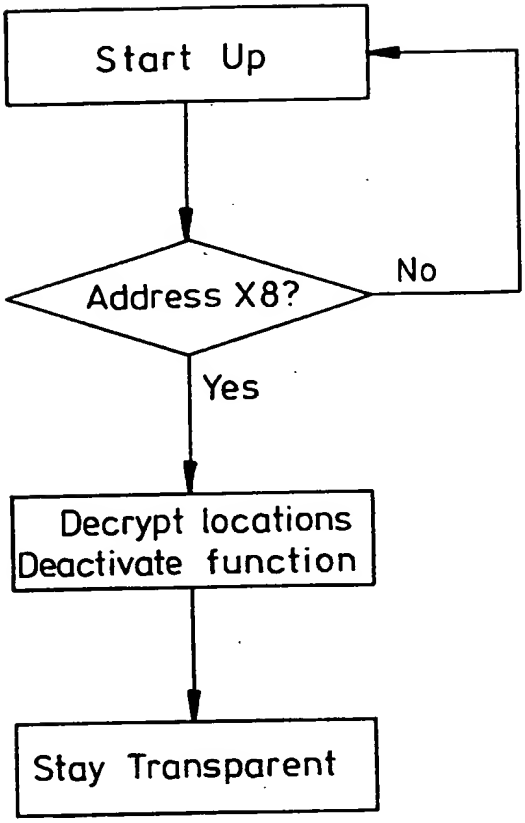
FIG. 2



Function 4)

Selective Data Encryption (Activation)

(for files or locations)



Function 4)

Selective Data Encryption (Deactivation)

FIG. 3

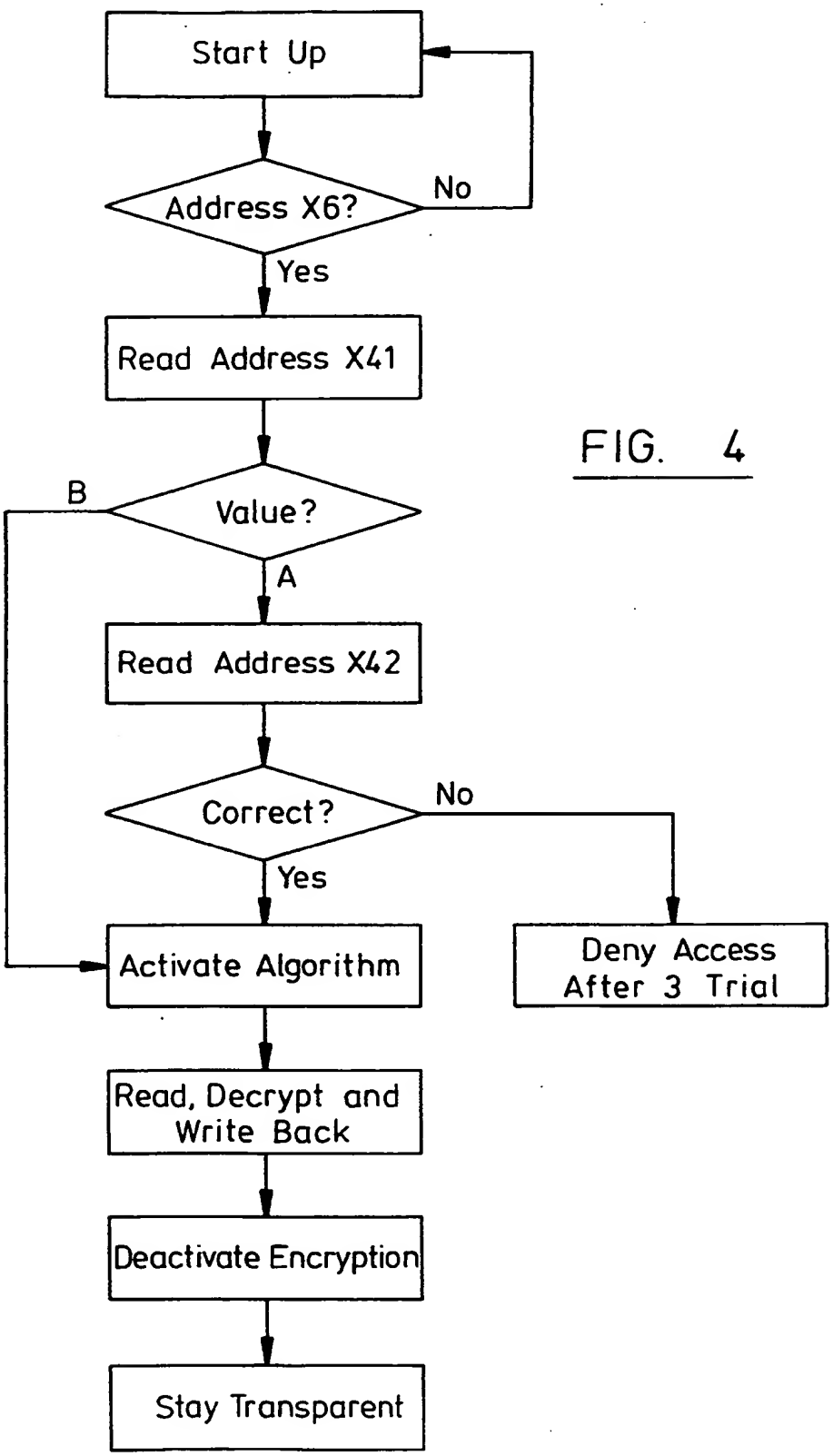
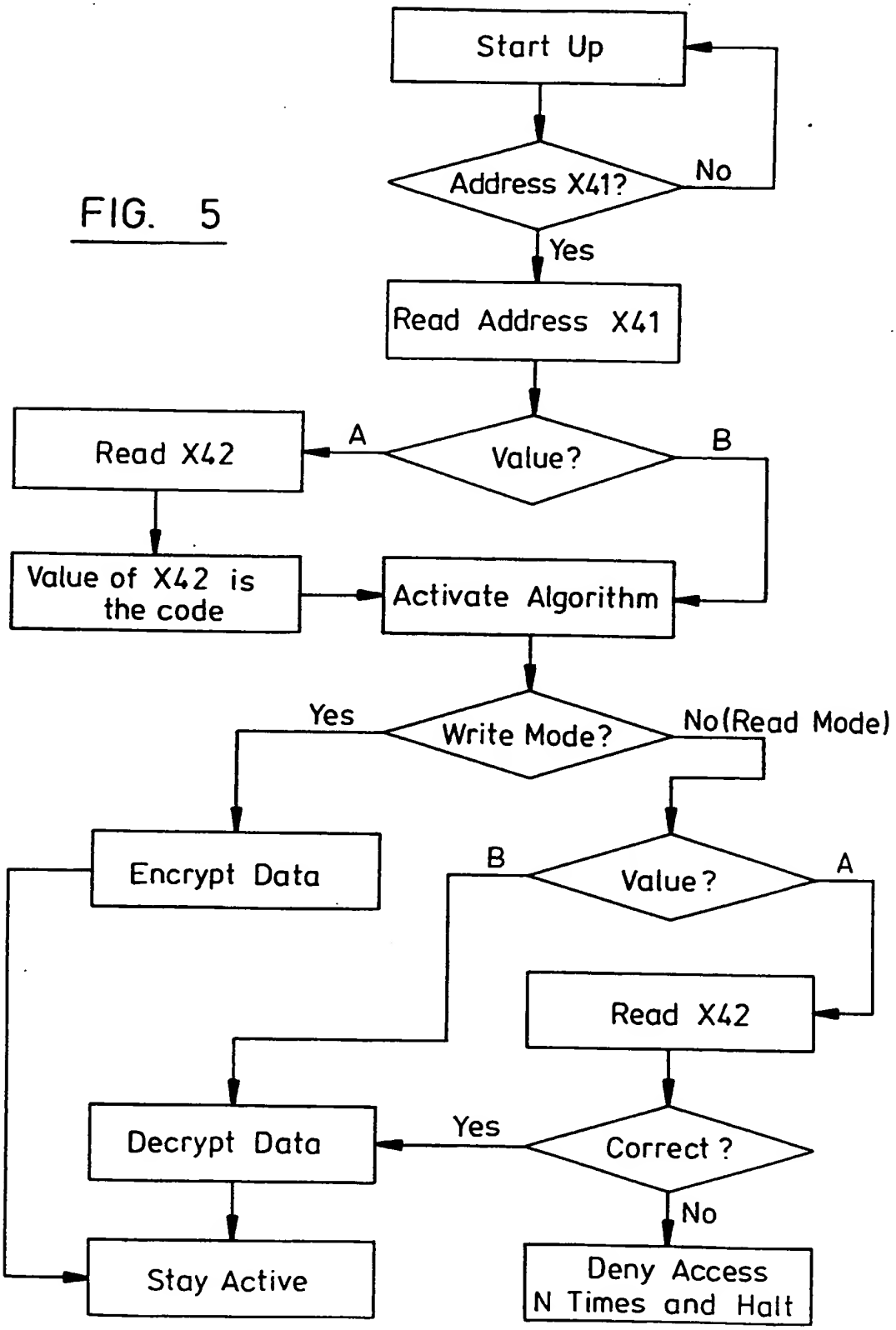


FIG. 4

Function 3)

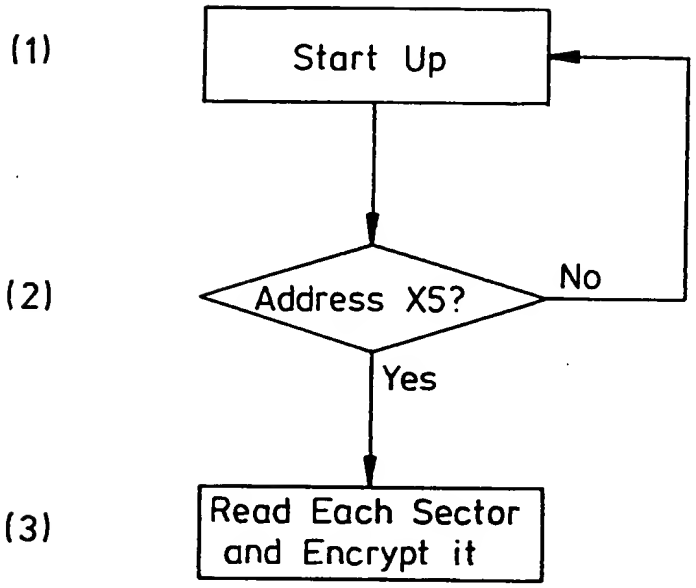
Data Encryption (Deactivation)

FIG. 5



Function 3)

Data Encryption (Activation)



Function 3)

Data Encryption (Initial Activation)

FIG. 6

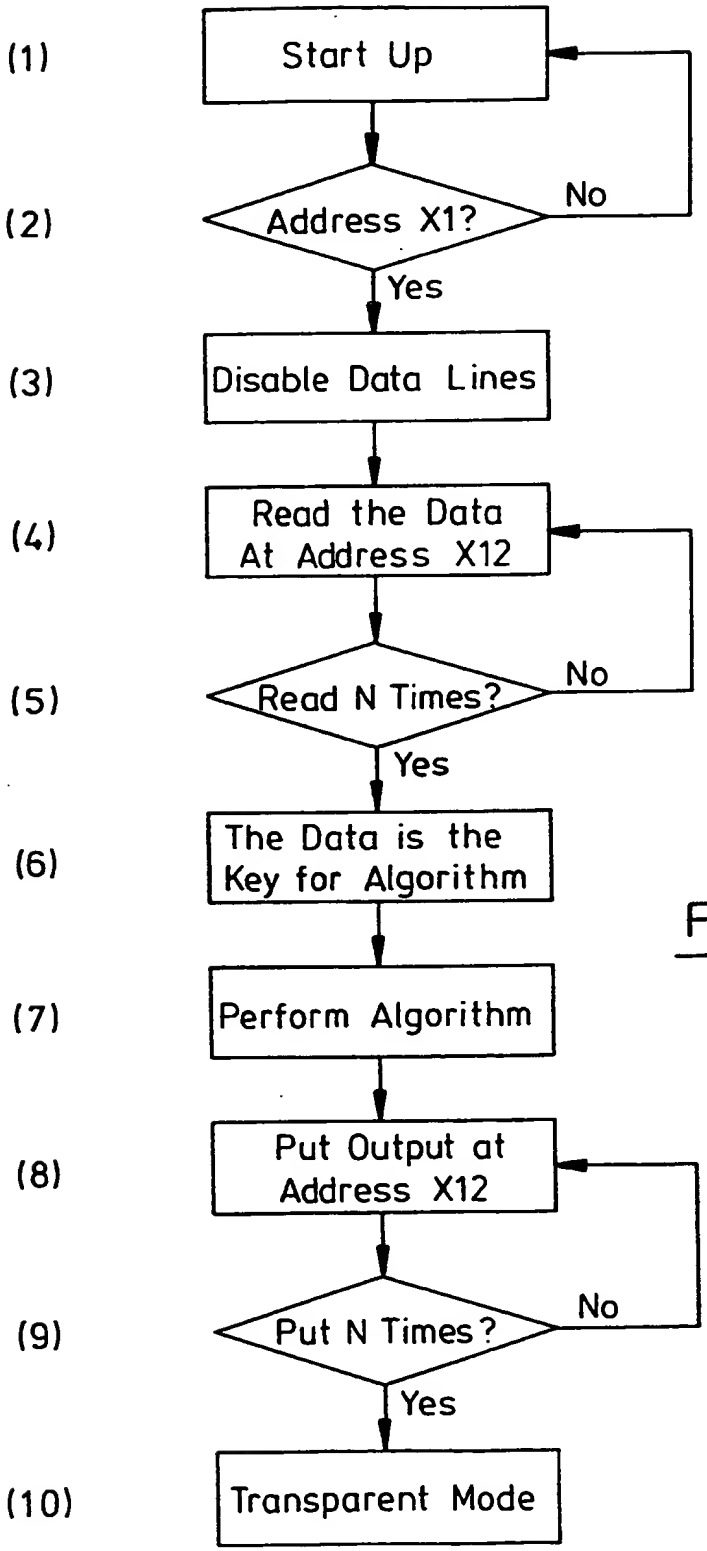
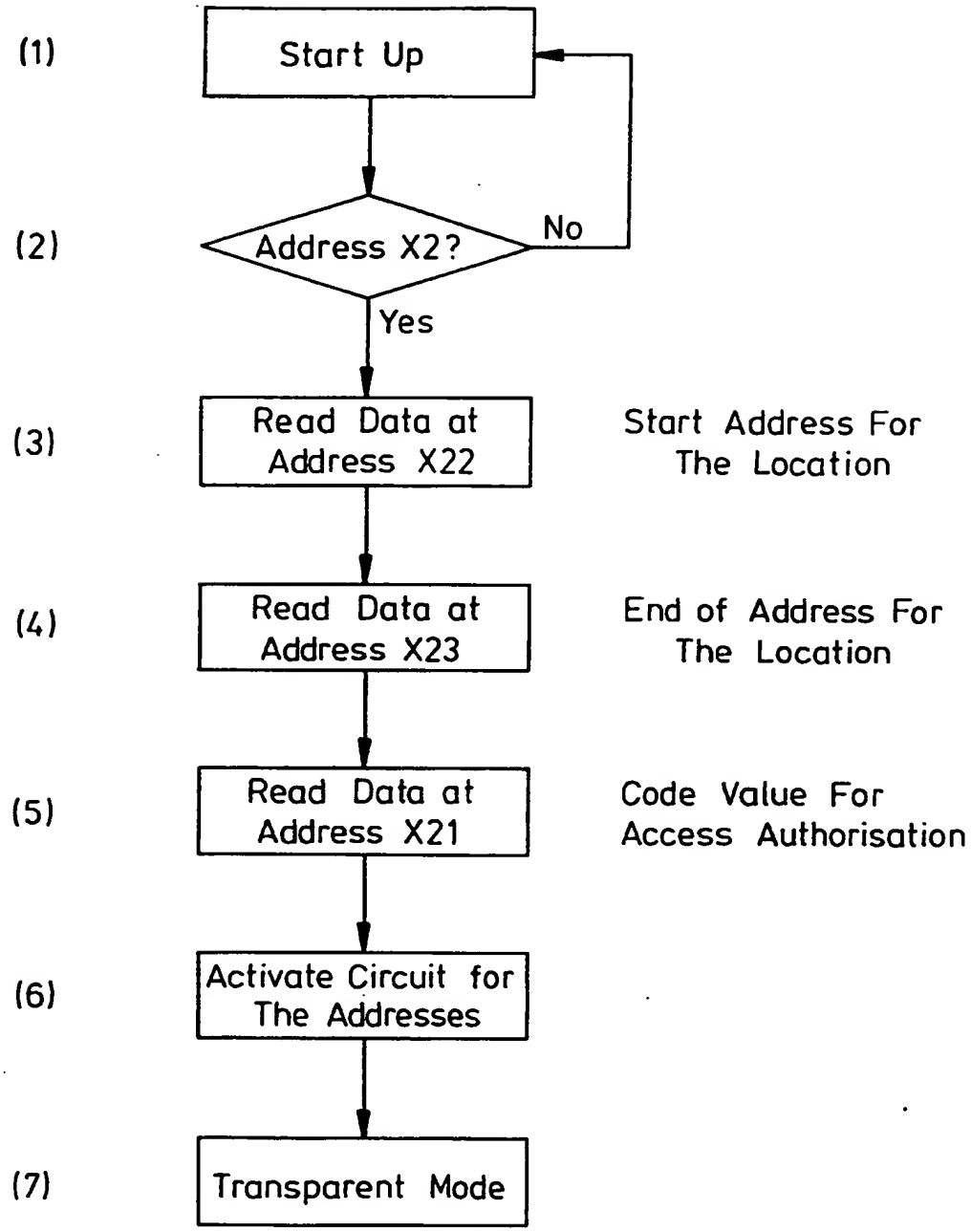


FIG. 7

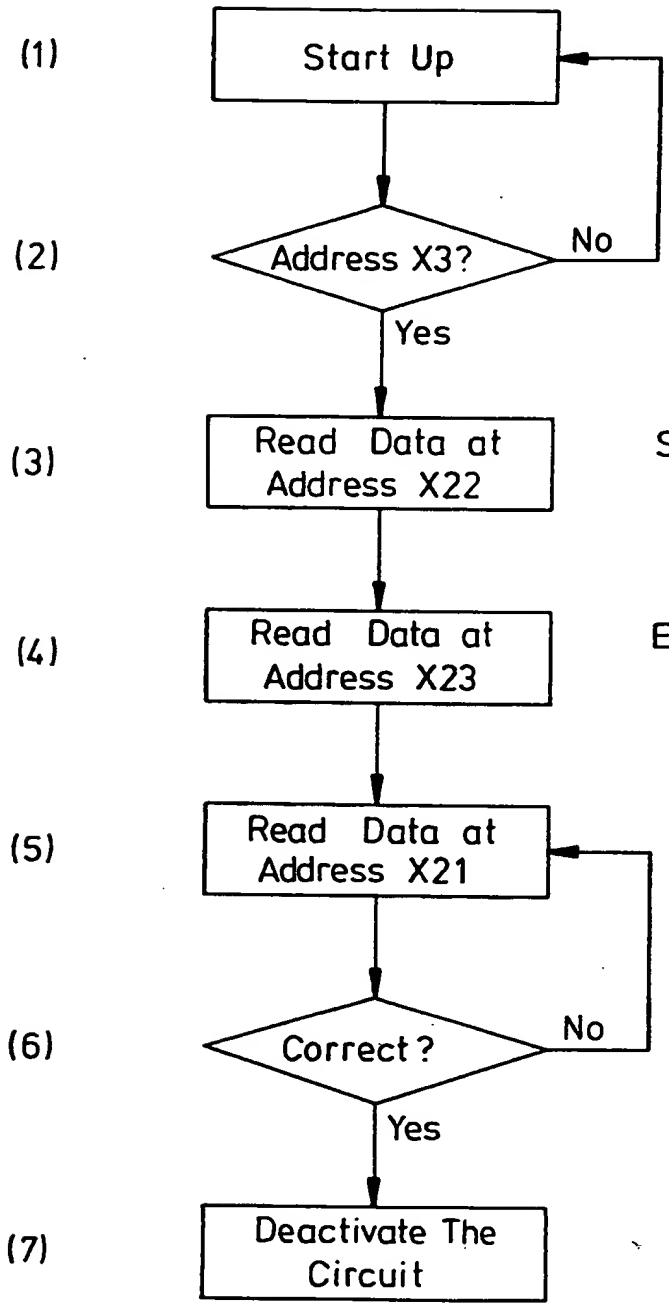
Function 1)

Algorithm Performing



Function 2)
Location Protection
a) Locking

FIG. 8



Function 2)
Location Protection
b) Unlocking

FIG. 9

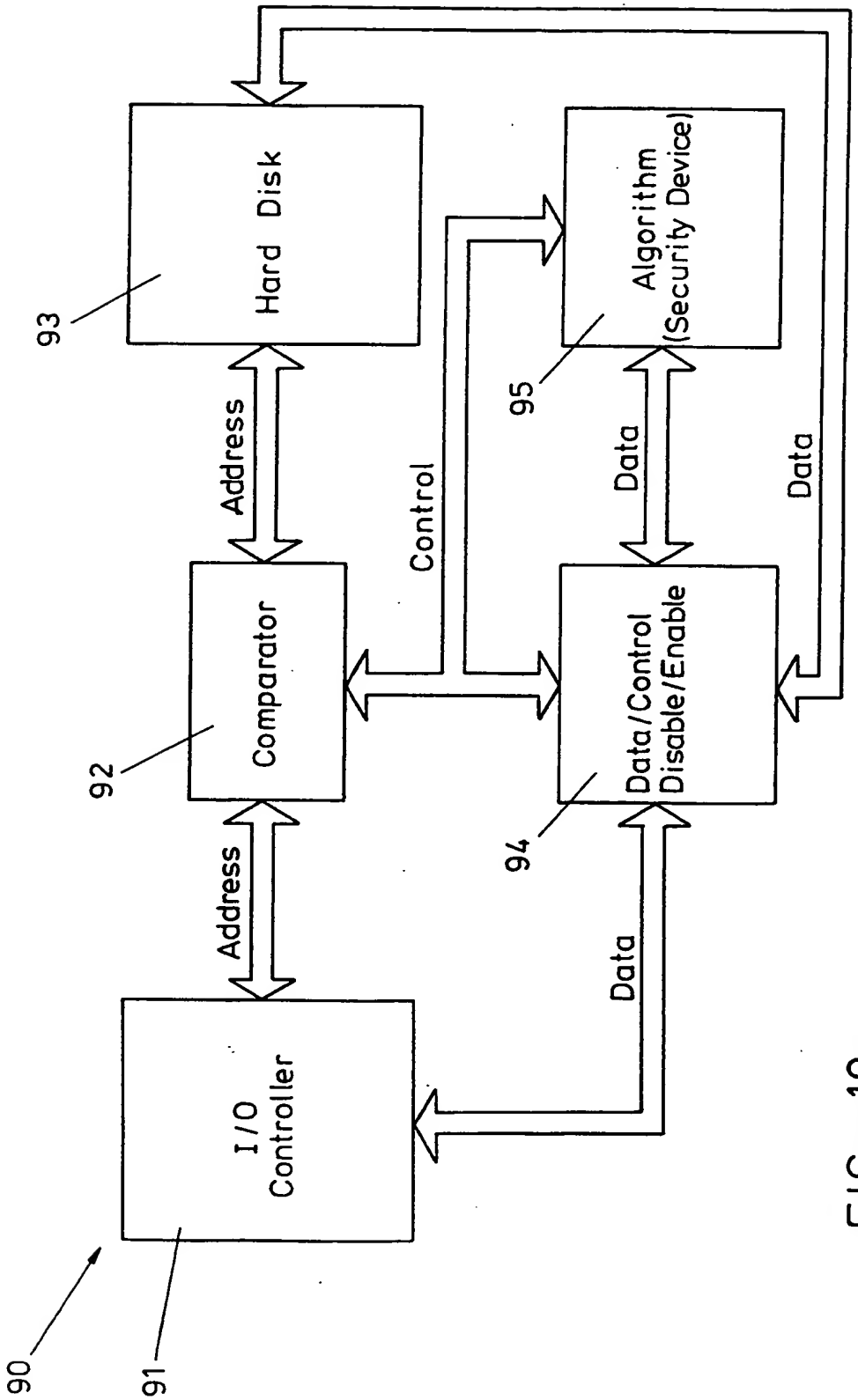

Hard Disk
93
Algorithm (Security Device)
95
Address
Control
Data
Data
Comparator
92
Data/Control Disable/Enable
94
Address
Data
I/O Controller
90
91

FIG. 10

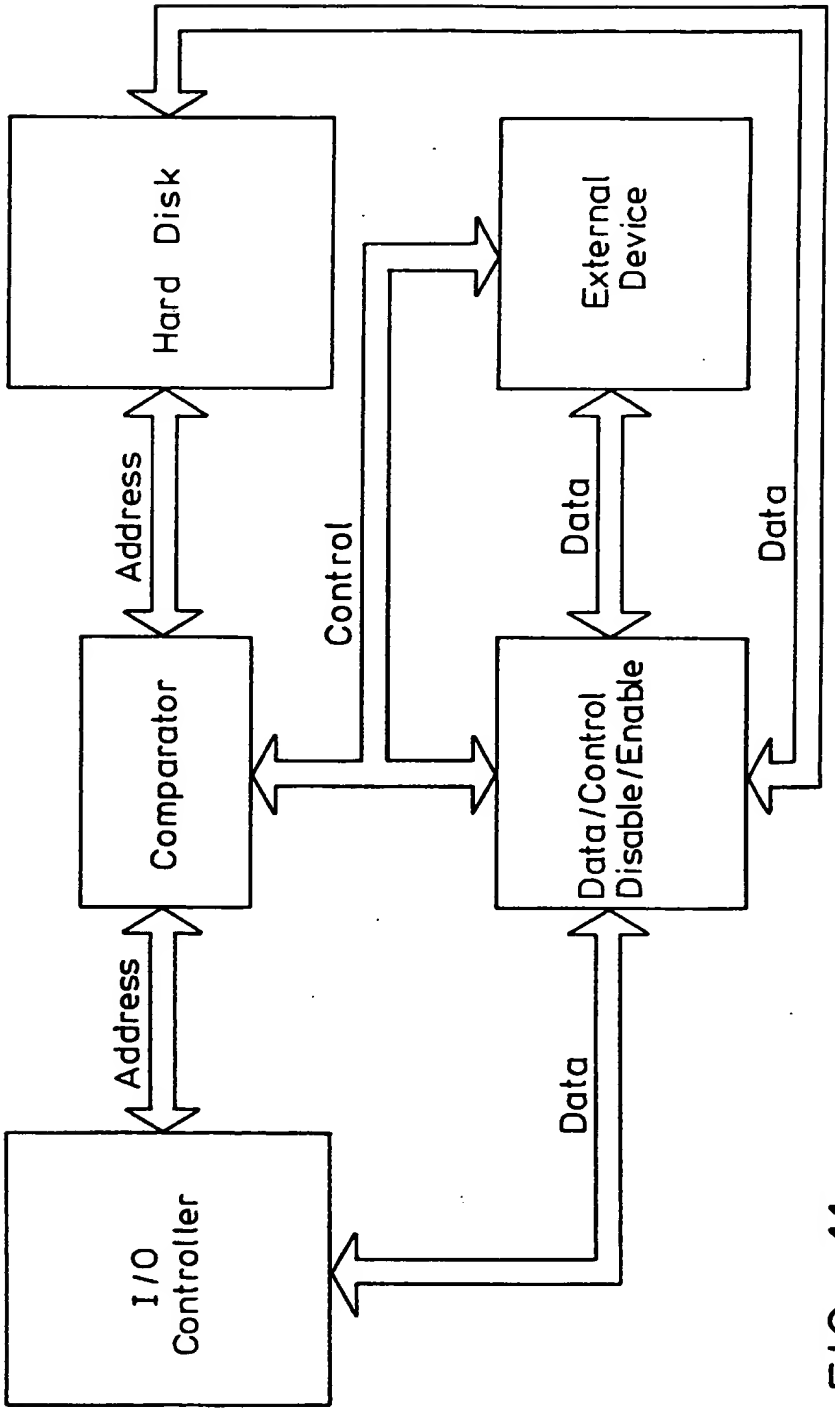

Hard Disk
External Device
Address
Control
Data
Data
Comparator
Data/Control
Disable/Enable
Address
Data
I/O
Controller

FIG. 11

INTERNATIONAL SEARCH REPORT

Intern al Application No
PCT/GB 93/01835

A. CLASSIFICATION OF SUBJECT MATTER
IPC 5 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 5 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US,A,5 033 084 (BEECHER) 16 July 1991	1,3,7,9, 10,12
A	see figures 1,7 see column 3, line 60 - column 4, line 59 see column 8, line 30 - column 9, line 14	6,11
X	WO,A,90 10292 (LIVOWSKY) 7 September 1990 see figures 1-4B see page 12, line 30 - page 13, line 8 see page 14, line 27 - page 19, line 8	1,3,7-12
A	EP,A,0 183 608 (SCHLUMBERGER TECHNOLOGY CORP.) 4 June 1986 see figures 1-3 see abstract see page 6, line 1 - page 7, line 9	1,4,7,9

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 January 1994	04. 02. 94

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	WEISS, P

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Interna. al Application No
PCT/GB 93/01835

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A-5033084	16-07-91	WO-A- 9115816	17-10-91
WO-A-9010292	07-09-90	FR-A- 2643475	24-08-90
		AU-A- 5173790	26-09-90
EP-A-0183608	04-06-86	JP-A- 61175729	07-08-86

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.